ITU Regional Training Workshop on IPv6 and IoT Strategy, Policy, and Implementation for Arab States 2022

IOT POLICIES AND STRATEGIES

Dr Navaneethan C Arjuman
ITU Expert

IOT POLICIES AND STRATEGIES

- IOT Challenges
- IOT Policies
- IOT Strategies

IOT CHALLENGES

Scalability

- A complex water monitoring systems which includes hundreds of midpoints and endpoints deployed over hundreds of kilometres is a very complex project than even the most complex consumer home automation projects.
- Since IoT systems can result in the generation of thousands datapoints, transmitting the information from the sensors to their base station should be considered (supervisory control and data acquisition (SCADA)) platform.

IOT CHALLENGES
CONT.

Cyber-Security Standards

- 70% of the most commonly used IoT devices encounter Cyber-security, according to Hewlett Packard research.
- Hacking smart home IoT devices could have important threat for personal privacy, however, the network intrusion would be local.
- However, in Industrial IoT systems where sensors sense critical infrastructure resources such as power plants and water management facilities the magnitude of the threat is much severe.

IOT CHALLENGES CONT.

Granularity

- Unlike sophisticated IoT products such as smart washing machines, IoT solutions need to be white-labelled and tailored to the individual usage requirements of the purchaser.
- Because of that, IoT solutions are available with a variety of means that are highly customized and can be integrated with other software systems. This includes APIs or Platform as a Service (PaaS) offerings.

IOT CHALLENGES CONT.

Security and data privacy

- Many wireless protocols such as WiFi, ZigBee, Z-Wave, and NB-IoT are supported, which allow different smart devices communicate with each other as well as a local gateway (e.g., a hub or a base station).
- Equipment used every day is marketed without taken into account issues like confidentiality or data protection.
- Many of us have accepted, voluntarily in our privacy and security to get what we consider more precious, namely, access to the cutting-edge technology.

IOT CHALLENGES CONT.

Tolerance to errors

- IoT world is more dynamic and mobile than the computers world, with contexts that change rapidly and in unexpected ways.

Interoperability

- Available energy and the bandwidth required for communications.

Managing large data volume

- Vritually any detail in user life can be taken as data that can be interpreted.

IOT CHALLENGES CONT.

Regulatory, legal, and rights Issues.

- IoT amplifies and reintroduces many regulatory and legal questions.
- There is a danger that the rapid rate of change in IoT technology could outpace the ability of associated policy, legal, and regulatory structures to adapt.
- One such issue includes the potential conflict between law enforcement surveillance and civil rights.

IOT POLICIES

Continuously improvement IoT Policies

- IoT devices will likely touch most aspects of our lives, including devices in our homes, workplaces, schools, hospitals, and other public spaces.
- As such, privacy, data security, healthcare, transportation, and technology and innovation policies will likely be impacted.
- This kind of broad reach suggests that policy makers will need to consider the broad policy implications across a wide field of policy goals and initiatives.

IOT POLICIES

- Government and stakeholders should continuously develop new policies that promote Internet infrastructure, efficient use of wireless spectrum, data-center development, and user empowerment and choice are critical to the evolution IoT.
- Ensuring lifetime security in IoT products and services must be a fundamental priority to maintain overall user trust in this technology.
- Users need to trust that IoT devices and related data services are secure, especially as they become more pervasive and integrated into our daily lives.

IOT STRATEGIES

Promote Internet and data-infrastructure growth.

- Governments should promote the expansion of both wireless and wireline infrastructure, including in rural and remote areas, and consider IoT needs for both licensed and unlicensed spectrum use.
- Barriers to data-center development and user-based systems for IoT data analysis, such as burdensome equipment taxes or licensing requirements, should be removed.
- Governments should review their existing Internet infrastructure in light of the potential increased data communication needs of IoT devices.

Source : https://www.internetsociety.org/policybriefs/iot/

IOT STRATEGIES CONT

Encourage IPv6 deployment.

- IPv6 is an enabling technology for Internet growth, and it will become even more critical as IoT drives up the number of connected devices.
- Governments should make IPv6 adoption a national priority and engage stakeholders in their community to encourage IPv6 rollout.

Source : https://www.internetsociety.org/policybriefs/iot/

IOT STRATEGIES CONT

Encourage open, voluntary IoT standards.

- Employing greater interoperability and the use of open, voluntary, and widely available standards as technical building blocks for IoT devices will support greater user benefits, innovation, and economic opportunity.
- Governments should refrain from mandating technical approaches to IoT, and, instead, encourage industry, researchers, and other stakeholders to work together on the development of open, consensus-based standards that support interoperability.

Source : https://www.internetsociety.org/policybriefs/iot/

IOT STRATEGIES CONT

Adopt a collaborative, multistakeholder approach to IoT policy discussions.

- IoT is a challenging area for policymakers, as it is a rapidly developing environment and its technology spans many industries and uses.
- A collaborative governance approach, one that draws on the expertise and engagement of a wide range of stakeholders, will be needed to develop effective and appropriate solutions.
- Policies should aim to promote users' ability to connect, speak, innovate, share, choose, and trust in a manner that both promotes innovation and enables user rights.

Source : https://www.internetsociety.org/policybriefs/iot/

IOT STRATEGIES CONT

Encourage a collaborative approach to IoT security.

- The Internet Society believes that IoT security is the collective responsibility of all who develop and use IoT devices.
- Participants in the IoT space should adopt a collaborative approach to security among its broad, multistakeholder community by assuming responsibility, sharing best practices and lessons learned, encouraging security dialog, and emphasizing the development of flexible, shared security solutions that can adapt and evolve as threats change over time.
- IoT security policy should focus on empowering players to address security issues close to where they occur, rather than centralizing IoT security among a few, while also preserving the fundamental properties of the Internet and user rights.

Source : https://www.internetsociety.org/policybriefs/iot/

IOT STRATEGIES CONT

Encourage responsible design practices for IoT services.

- Security-by-design and privacy-by-design practices for IoT devices should be encouraged.
- Whether via privacy and data protection regulation, voluntary industry self-regulation, or other incentives or policy means, IoT device developers should be encouraged to respect the end-user's privacy and data security interests and consider those interests a core element of the product-development process.
- IoT system designers also should consider the full lifecycle of the IoT system to ensure obsolete devices don't pose security risks and are compatible with responsible environmental stewardship.

Source : https://www.internetsociety.org/policybriefs/iot/

Q & A